ВІДГУК

офіційного опонента на дисертаційну роботу

Бистрової Богдани Василівни

„Професійна підготовка бакалаврів з кібербезпеки

у вищих навчальних закладах США”,

подану на здобуття наукового ступеня кандидата педагогічних наук

зі спеціальності 13.00.04 – теорія і методика професійної освіти

Актуальність теми дисертаційної роботи.

Проблеми захисту відомостей, даних, інформаційних об’єктів, що формуються, циркулюють і використовуються у різних сферах людської діяльності, тою чи іншою мірою існувала завжди – практично з часів виникнення людської цивілізації. В останні часи вони суттєво загострилася через глобалізацію світових процесів суспільного розвитку, поглиблення конкуренції на світових економічних ринках, прискорення науково-технічного прогресу, погіршення екологічної ситуації в локальному і планетарному масштабах, інформатизацією всіх сфер людської діяльності, зокрема, блискавичного і всеохоплюючого поширення комп’ютерно орієнтованих засобів діяльності людини та інформаційно-комунікаційних технологій (ІКТ) різного предметного призначення, створення потужних баз електронних даних та пошуково-навігаційних засобів інформаційних об’єктів, глобальних систем електронних комунікацій на базі спеціалізованих інформаційно-комунікаційних мереж (ІКМ) та мережі Інтернет. Ці інформаційні системи, засоби і технології, опрацьовуючи і розповсюджуючи інформаційні об’єкти, не тільки позитивно впливають на характер функціонування і продуктивність програмно-технічних систем, на підвищення ефективності функціонування соціо-технологічних систем та здійснення будь-якої інформаційно-комунікаційної діяльності (ІК-діяльності) людини, на якісне розв’язання нею професійних і побутових проблем, але й

негативно „втручаються” як у функціонування різних техніко-технологічних систем, так і у діяльність людини, тобто у функціонування соціо-технологічних систем, непоодиноко суттєво ускладнюючи і, навіть, унеможливлюючи функціонування систем і діяльність людини, або спрямовуючи ці функціонування і діяльність у небажаний бік. В останній час це «втручання» поглиблюється через суттєве посилення впливу інформаційного фактору на характер проведення гібридних військових дій. Певною мірою через це у 2016 році 28 країн НАТО оголосили кіберпростір операційною зоною, поряд з повітрям, сушею та морем.

Таким чином, захист даних в інформаційних системах (ІС) сьогодні виокремився у специфічну складну проблему, успішне розв’язання якої, не тільки дозволяє підвищити ефективність функціонування комп’ютерно орієнтованих систем, але й сприяє розширенню спектру їх практичних застосувань.

Це стосується також і системи освіти (СО), передусім відкритої освіти, де ІКТ-системи та ІКМ утворюють її комп’ютерно-технологічну платформу. Через це комп’ютерно орієнтовані системи освіти, передусім їх змістово-технологічні складники, стають потенційно вразливими від несанкціонованих втручань і непрофесійних дій.

Це зумовлює порушення цілісності баз даних різних ІС – інформаційних баз (ІБ), що проявляється у викривленні змісту інформаційних об’єктів (ІО), або їх повної втрати, змінах структури відношень між ними, тобто порушенні будови баз даних ІС, а отже і до втрати користувальних властивостей ІС в цілому. Деякі несанкціоновані втручання і непрофесійні дій відносно баз даних ІС можуть також виводити з працездатного стану програмне забезпечення ІС і навіть руйнувати на фізичному рівні ІКТ-інфраструктуру, що підтримує ІС.

Причини, за яких відбувається порушення цілісності ІБ з боку джерел їх виникнення, можуть бути як навмисними, так і ненавмисними. До ненавмисних відносяться причини, пов’язані з непрофесійними діями персоналу, що обслуговують системи опрацювання даних (СОД), а також непередбачувані

причини суто техніко-технологічного характеру (вихід з ладу засобів СОД, зрив постачання електроенергії, форсмажорні обставини та ін.).

Навмисні порушення цілісності ІБ відбуваються як наслідки (причини) цілеспрямованої діяльності осіб (професійних груп), які:

- розробляють і розповсюджують через ІКМ програмні агенти, що змінюють інформаційний контент та склад ІО баз даних, вносять до них додаткові ІО або вкрапляють у існуючи ІО небажаний для потенційного користувача зміст, в тому числі, повністю чи частково його руйнують;
- розробляють і розповсюджують через ІКМ програмні агенти, що змінюють структуру баз даних, вносять до неї додаткові небажані або неприпустимі зв'язки, в тому числі, повністю чи частково руйнують структуру баз даних;
- здійснюють або намагаються здійснити несанкціонований доступ до ІО існуючих інформаційних баз з обмеженим доступом, зокрема, з метою викрадення відомостей обмеженого користування.

Перша із зазначених вище причин порушення цілісності ІБ зумовлює викривлення свідомості людей, впливає на їхню обізнаність щодо реального стану речей, на усвідомлені та сформовані ціннісні системи, на стабільність їхньої індивідуальної психіки і, як результат, на поведінку людей у тих чи інших життєвих ситуаціях. Зокрема, ця причина суттєво вливає на функціонування систем прийняття рішень в організаційних системах, коли навіть незначні порушення цілісності ІБ можуть призвести до значних і, навіть, непоправних помилок, подій і, навіть, трагедій глобального масштабу. Це стосується також ерготичних систем, до елементного складу яких обов'язково входить людина або група людей, а прийняття рішень переважно відбувається у нестандартних ситуаціях.

Друга з цих причин, означається як кіберзлочинність і карається відповідно до чинного законодавства. Третя – безпосередньо пов'язана з дотриманням

таємниць державного, науково-технічного та фінансово-економічного характерів, національної безпеки країн. У разі її практичного застосування з використанням комп'ютерно орієнтованих засобів та ІКТ, ця причина теж, як і дві перші із зазначених, відноситься до кіберзлочинності і є предметом кримінального права.

Вочевидь, що усвідомлюючи ризики, пов'язані із загостренням зазначених проблем, світове суспільство висуває і буде надалі висувати все більш і більш високі вимоги до ступеня захищеності даних в ІКМ і комп'ютерно орієнтованих системах, до рівня інформаційної безпеки окремих громадян, їх соціальних спільнот, держав, країн і світу в цілому.

Багато в чому розв'язання третьої із зазначених проблем, запобігання й нейтралізація загроз, зниження ризиків порушення цілісності ІБ, досягнення необхідного рівня інформаційної безпеки залежить від якості підготовки фахівців, які забезпечують інформаційну безпеку формування і використання комп'ютерно орієнтованих ІБ, в тому числі, ІБ з обмеженим доступом.

Як правильно зазначає авторка дисертації (ст.6 автореферату) «Вивчення наукового доробку вітчизняних і зарубіжних науковців і практиків засвідчило, що професійна підготовка фахівців з кібербезпеки є одним із складників національної безпеки…»

Розглядаючи освітні аспекти розв'язання проблем інформаційної безпеки та кібербезпеки в США, доцільно вказати на основні важливі аспекти міжнародної стратегії США з цих питань, які варто включити у зміст підготовки фахівців з кібербезпеки.

Зокрема, в «Міжнародній стратегії США для кіберпростору» вказується, що ця стратегія: «… повністю відповідає думці про те, що відповідні міжнародні норми мирної поведінки та розв'язування конфліктів цілком застосовні і у кіберпросторі … Ці норми варто прив'язати до традиційних принципів підтримування фундаментальних свобод, поваги права приватної власності, права на збереження таємниці приватних даних, права на захист від правопорушників, а

також права на застосування засобів самозахисту». Саме на цьому грунті стоять такі міжнародні норми як: глобальна сумісність систем, стабільність мереж, надійний доступ до мережних ресурсів, багатостороннє управління, забезпечення безпеки зусиллями держав (https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti).

У лютому 2003 року в США було оприлюднено «Національну стратегію досягнення безпеки у кіберпросторі» (*"National Strategy to Secure Cyberspace"*), в якій сформульовані п’ять пріоритетів діяльності США із забезпечення інформаційної безпеки, а також основні завдання в межах цих пріоритетів на середньострокову і довгострокову перспективу. У цьому документі до основних державних пріоритетів віднесено: 1. Становлення і розвиток національної системи реагування на події у сфері інформаційної безпеки; 2. Реалізація комплексної системи заходів із зменшення загроз у сфері інформаційної безпеки; 3. Забезпечення підготовки спеціалістів у сфері комп’ютерної безпеки та відповідального ставлення всього населення країни до питань захисту інформації; 4. Забезпечення захисту інформаційних систем, що мають відношення до державних органів; 5, Розвиток різних форм кооперації (у тому числі і міжнародної) у сфері інформаційної безпеки (https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0;).

Варто також навести основні терміни і поняття, що подані у загальнодоступних джерелах (дещо уточнені) і без розуміння яких складно аналізувати зміст цієї роботи (https://www.intuit.ru/studies/courses/563/419/lecture/9576; https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%B

E%D1%81%D1%82%D1%8C_(%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%B8%D1%8F).

Передусім це поняття *інформаційної безпеки* (ІБ), яке можна подати з різних, проте суттєвих і взаємодоповнюючих точок зору: по-перше, ІБ – захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного чи штучного характеру, що можуть нанести збитки власникам або користувачам інформації чи підтримуючої інфраструктури; по-друге, ІБ – стан (якість) певного об'єкта; по-третє, ІБ – діяльність, спрямована на забезпечення захищеного стану об'єкта; по-четверте, ІБ – галузь знань з напряму «Комп'ютерні науки», в межах якої ведеться певна науково-освітня діяльність; по-п'яте, ІБ – дисципліна (цикл дисциплін) та навчальна програма (низка програм), в межах яких і за якими здійснюється освітня діяльність.

Інформаційна безпека держави – стан збереження інформаційних ресурсів держави та захищеності законних прав громадян і суспільства в інформаційній сфері (https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).

Поняття *кібербезпека* (КБ), теж можна подати з різних, проте суттєвих і взаємодоповнюючих точок зору: по-перше, КБ – розділ ІБ, в межах якого вивчаються процеси формування, функціонування та еволюції кібероб'єктів; по-друге, КБ – заходи з безпеки, що застосовуються для захисту обчислювальних пристроїв, а також комп'ютерних інформаційно-комунікаційних мереж; по-третє, КБ – простір діяльності системних адміністраторів, що охоплює усі засоби, процеси і механізми, за допомогою яких забезпечується КБ комп'ютерно орієнтованих систем; по-четверте, КБ – процес використання заходів безпеки для забезпечення конфіденційності, цілісності та доступності даних

(https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0;
https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).

Оскільки в США, як технологічно передової країни світу, накопичений значний, за оцінками багатьох фахівців – найбільший, науково-практичний та освітній досвід з питань кібербезпеки, то вивчення цього досвіду, передусім досвіду навчання, підготовки та перепідготовки спеціалістів з кібербезпеки, може бути надзвичайно корисним для України, що крокує у напрямі цифрової трансформації суспільства з деяким запізненням.

Розв’язання завдань дисертаційної роботи Б.В. Бистрової сприяє вирішенню важливої наукової проблеми та полягає в аналізі наявного досвіду США з питань кібербезпеки, передусім в освітній сфері, та розробленні рекомендацій щодо використання цього освітнього досвіду в системі професійної підготовки у вищих закладах освіти України бакалаврів з кібербезпеки.

Зважаючи на викладене вище, тему дисертаційного дослідження Б.В. **Бистрової** „Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США”, яка саме і присвячується дослідженню освітніх проблем забезпечення кібербезпеки, можна визнати актуальною, а її розроблення – своєчасним.

Дисертація виконана в Інституті педагогічної освіти і освіти дорослих Національної академії педагогічних наук України.

Актуальність теми дисертації підтверджується також тим, що її дослідження проведено відповідно до тематичного плану науково-дослідної роботи Інституту

педагогічної освіти і освіти дорослих НАПН України за темою «Тенденції розвитку освіти дорослих у розвинених країнах світу» (РК № 0117U001070).

Тему дисертаційного дослідження затверджено вченою радою Інституту педагогічної освіти і освіти дорослих НАПН України (протокол №1 від 30 січня 2017 р.) та узгоджено у Раді з координації наукових досліджень у галузі педагогічних і психологічних наук України (протокол № 3 від 16 травня 2017 р.).

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Ця ступень є достатньою і забезпечена обраною методологічною базою дослідження, яку становлять провідні положення компаративістичних досліджень на основі діахронічного і синхронічного вивчення педагогічних, соціально-культурних та економічних реалій, а також коректним застосуванням комплексу взаємодоповнюючих методів дослідження: теоретичних, емпіричних, прогностичних, зокрема, методів узагальнення та класифікації психолого-педагогічних джерел і передових освітніх практик, загальних методів пізнання (спостереження, порівняння, класифікація), опитувально-діагностичних методів (тестування, опитування, вимірювання) та обсервації (анкетування, інтерв'ювання, бесіда).

Виявлення особливостей професійної підготовки бакалаврів з кібербезпеки у вищих закладах освіти США і України проведено з урахуванням сукупності критеріїв: нормативно-правового, змістового, організаційного, технологічного, що забезпечують їх обґрунтованість.

Загальні висновки випливають зі змісту роботи, у концентрованому вигляді відображають основні результати дослідження відповідно до його завдань. У роботі зроблені необхідні узагальнення й висновки.

Апробація результатів дослідження, повнота їх викладу в опублікованих працях.

Отримані в дисертації результати протягом 2005 – 2018 років оприлюднено та обговорено на 10 міжнародних та всеукраїнських наукових, науково-практичних та науково-методичних конференціях, що проходили як в Україні, так і за кордоном, та на 4 звітних наукових конференціях Інституту педагогічної освіти і освіти дорослих НАПН України.

Ці результати з необхідною повнотою викладено у 15 публікаціях, з них: 6 статей у фахових виданнях України, у т.ч. 1 – у виданні України, що включено до міжнародних наукометричних баз; 1 стаття у зарубіжному науковому періодичному виданні; 1 методичні рекомендації; 7 публікацій у збірниках матеріалів науково-практичних конференцій.

Ознайомлення зі змістом публікацій Б.В. Бистрової свідчить про повноту викладу основних результатів дисертації, які одержав здобувач, у наукових фахових виданнях, що відповідає п.12 „Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника”.

Структура та обсяг дисертації.

Дисертаційна робота складається зі вступу, трьох розділів, висновків до кожного розділу, загальних висновків, списку використаних джерел, що включає 347 найменування, з них 177 – іноземними мовами, та додатків на 43 сторінках. Загальний обсяг дисертації становить 244 сторінки друкованого тексту, з них 182 сторінки – основний текст. Робота містить 14 рисунки та 13 таблиць.

Оформлення дисертації в цілому відповідає чинним вимогам.

Аналіз змісту дисертаційного дослідження

У *вступі* дослідницею обґрунтовано актуальність обраної теми; відображено зв’язок роботи з вітчизняними науковими програмами, планами і темами; сформульовано мету і завдання дослідження; окреслено його об’єкт, предмет і методи; сформульовано наукову новизну та практичне значення роботи; подано відомості про апробацію результатів, публікації, структуру й обсяг дисертації.

У *першому розділі* схарактеризовано стан дослідженості проблеми професійної підготовки фахівців з кібербезпеки у педагогічній і науково-методичній літературі; визначено основні поняття дослідження; проаналізовано підходи до професійної підготовки фахівців з кібербезпеки у документах міжнародних організацій.

З'ясовано, що в умовах інформаційних війн, замахів на цілісність і суверенітет держави проблема підготовки фахівців з кібербезпеки є не лише педагогічною, а й системною, міждисциплінарною. На основі аналізу нормативно-правових документів міжнародних організацій матеріалів міжнародних конференцій з питань захисту кіберпростору тощо, з'ясовано вимоги ЄС до забезпечення його глобального, відкритого, безпечного характеристик.

У *другому розділі* проаналізовано положення Національної стратегії професійної підготовки фахівців з кібербезпеки; виявлено соціально-економічні та політичні чинники впливу на професійну підготовку майбутніх фахівців з кібербезпеки; викладено загальну характеристику системи професійної підготовки бакалаврів з кібербезпеки у вищих закладах освіти США; визначено можливі освітні траєкторії неперервної освіти американських ІТ-фахівців.

З'ясовано, що Національна стратегія США щодо удосконалення інформаційної безпеки, задоволення кількісних та якісних вимог ринку праці до професійної підготовки кадрів з кібербезпеки реалізується шляхом виконання середньострокових та довгострокових завдань. Виявлено чинники впливу на розвиток та становлення американської системи професійної підготовки фахівців з кібербезпеки. Проаналізовано основні принципи організації вищої освіти США. Виявлені диверсифіковані освітні траєкторії здобуття освіти та охарактеризовано систему неперервної професійної підготовки фахівців з кібербезпеки в США, що функціонує на засадах відкритості, гнучкості, варіативності, послідовності та спадкоємності засвоєння знань, їх постійного вдосконалення та оновлення відповідно до потреб практики.

У *третьому розділі* визначено змістові та структурно-організаційні особливості теоретичної і практичної підготовки бакалаврів з кібербезпеки у вищих закладах освіти США; схарактеризовано форми і методи організації освітнього процесу бакалаврів з кібербезпеки; виявлено рівні забезпечення якості підготовки бакалаврів з кібербезпеки в американських закладах вищої освіти.

Аналіз освітньо-професійних програм підготовки у 45 американських вищих закладах освіти з 25 штатів США дозволив виявити змістові і структурно-організаційні особливості організації професійної підготовки бакалаврів з кібербезпеки. Вивчення навчальних програм вищих закладів освіти США дозволило виявити та узагальнити обов'язкові вимоги до організації підготовки фахівців для ІТ-галузі зі спеціальності «Кібербезпека». З'ясовано, що практична підготовка бакалаврів з кібербезпеки здійснюється в органах силових структур і державного управління, промислової і банківської сфери, в яких студенти оволодівають необхідними професійними навичками та уміннями. Схарактеризовано шляхи підвищення якості професійної підготовки фахівців із кібербезпеки. Виявлені умови постійного вдосконалення діяльності вищих закладів освіти США, однією з яких є проведення аудиторських перевірок. Подано загальну характеристику процедури зовнішнього оцінювання американських вищих закладів освіти, визначальними рисами якої є добровільна основа проходження акредитації, самостійне прийняття рішення щодо її необхідності.

У *четвертому розділі* розглянуто сучасний стан підготовки бакалаврів з кібербезпеки у закладах вищої освіти України; здійснено порівняльно-педагогічний аналіз особливостей професійної підготовки бакалаврів з кібербезпеки в США та Україні; з'ясовано можливості творчої реалізації конструктивних ідей американського досвіду в системі вищої освіти України.

Проведений аналіз освітньо-професійних програм, навчальних планів професійної підготовки бакалаврів за спеціальністю «Кібербезпека» українських

закладів вищої освіти. Доведено, що в практичній підготовці бакалаврів з кібербезпеки в українських закладах вищої освіти бракує інтегративного підходу з метою поєднання навчання в університеті та здобуття практичних умінь на майбутньому потенційному робочому місці; спостерігається недостатньо налагоджене соціальне партнерство із можливими роботодавцями для оволодіння практикантами необхідними знаннями з фаху. За результатами порівняльно-педагогічного аналізу професійної підготовки бакалаврів з кібербезпеки у закладах вищої освіти України і США обґрунтовано науково-методичні рекомендації щодо використання конструктивних ідей американського досвіду в українських реаліях на таких рівнях: стратегічному, організаційному, змістовому.

Зауваження до змісту дисертації.

Вважаю за необхідне висловити деякі зауваження до дисертації та побажання її автору:

1. Непоодиноко в роботі терміни „компетенція” і „компетентність” використовуються некоректно. Ці поняття мають бути чітко розведені, а їх застосовування повинно відповідати їх тлумаченню в сучасних останніх енциклопедичних і наукових джерелах.

2. При аналізі педагогічних умов професійної підготовки майбутніх фахівців з кібербезпеки в США варто було б показати, як використання в навчально-виховному процесі сучасних засобів навчання, передусім мобільних Інтернет-пристроїв, впливає на характер реалізації і перспективи розвитку педагогічних систем професійної підготовки бакалаврів з кібербезпеки і як це можна використати в Україні при вдосконаленні відповідних освітніх систем.

3. У зв’язку з тим, що за сучасних умов якісну професійну підготовку майбутніх фахівців інформаційної безпеки можливо здійснювати у відкритих педагогічних системах, коли учасники навчально-виховного процесу активно використовують інформаційні ресурси освітньо-просторової компоненти відкритого електронного освітнього простору, в роботі було б доцільно окремо

проаналізувати специфіку побудови і функціонування відкритих методичних систем професійної підготовки бакалаврів з кібербезпеки у вищих навчальних закладах США, тобто відповісти на питання – як методи, моделі, електронні освітні ресурси та педагогічні технології формування професійних компетентностей майбутніх фахівців з кібербезпеки в процесі їхньої підготовки відповідають принципам відкритої освіти, що відображають освітню парадигму рівного доступу до якісної освіти.

4. На с.26 і с.27 дисертації авторка наводить та описує деяку модель *інформації*, яку на рис 1.1 називає «чотири складові інформації та взаємозв'язок між ними», а в тексті – «структура поняття інформації». Насправді поняття інформації є дуже складним, і дотепер у професійному середовищі остаточно не визначеним. Оскільки авторка не посилається на джерело, де пропонується ця модель, складається враження, що ця модель запропонована авторкою. Проте, незрозумілою є сама мета подання у дисертації цієї моделі, а її склад і структура викликають багато запитань, відповіді на які в роботі відсутні. Наприклад, по-перше, за якими критеріями виконана декомпозиція моделі на компоненти (складники), оскільки, якщо такі критерії не вказано, компонентів може бути скільки завгодно (як за призначенням, так і за кількістю); по-друге, взаємозв'язок компонентів не наведено, отже структура поняття *інформації* відсутня, а назва рисунку не відповідає його змісту; по-третє, авторка не визначає, а тому залишається не зрозумілим, який чинник у запропонованій моделі відіграє системоутворювальну роль, що дозволяє розглядати поняття *інформації* та його модель як цілісність, та ін.

5. Незрозуміло, чому на рис 3.2 (с.154), який у роботі називається *характеристика напрямів комплексної практичної підготовки*, авторка обирає концентричну модель її подання, яка своєю геометрією передбачає, що всі наступні шари моделі охоплюють попередні і мають більший обсяг (площу кільця). Тай й ніяких характеристик усіх зазначених видів практичної підготовки

на рисунку не наводиться, тобто, назва рисунку одна, а зміст – інший.

6. Значною мірою п’яте зауваження стосується і рис 1.5, який названо «Провідні технології у кадровому забезпеченні ІТ-галузі (спеціальність «Кібербезпека»). Як вказано на с.58 – «джерело: самостійне опрацювання автора». Проте ніякі технології на рисунку не наводяться, а склад компонентів не обґрунтовується і не узгоджується з текстом, що слідує за цим рисунком.

7. На рис. 2.1 (с. 77) наведено «Структуру системи освіти США». Як вказано на с.78 – «джерело: систематизовано автором». По-перше, варто було б пошукати джерела, де така структура, поза сумніву, наводиться та описується. По-друге, у тексті, що безпосередньо слідує за цим рисунком (с.78), вказано «Особливості державного устрою США визначають відсутність єдиної системи освіти…». Що ж тоді будує авторка? По-третє, на рисунку відсутні зв’язки з усіма виділеними авторкою компонентами системи освіти США, через це, за підходом авторки, повна структура системи відсутня, а освіта США не може вважатися системою.

8. Матеріал, наведений у розділі 3.3 та загальних висновках по роботі, мав би бути більш масштабним і конкретним та включати, орієнтовані на певні органи управління освітою (загальнодержавні та місцевого самоврядування), на заклади вищої освіти (державні і приватні), можливо, на громадські структури суспільства України, системні та практично спрямовані пропозиції (подані у якісних і кількісних вимірниках, а також у формі рекомендацій з удосконалення законодавчо-правової бази) щодо побудови і вдосконалення системи підготовки бакалаврів з кібербезпеки, а можливо і на наступність перспективної підготовки в Україні магістрів з кібербезпеки, нагальна потреба у якій безсумнівно існує.

9. Відсутній взаємозв'язок між списком використаних джерел та цитованими фрагментами тексту, а також посиланнями на міжнародні та вітчизняні нормативні документи, закони, стратегії та ін.

10. В тексті дисертації та автореферату зустрічаються окремі граматичні та синтаксичні помилки та некоректне використання деяких термінів, наприклад,

замість правильного мережних – мережевих (с.9, с.11 авт, с.39 та ін. всюди по тексту), замість правильного змістова – змістовна ємність (с.47); замість правильного формування у фахівців компетентностей – надання необхідних знань та навичок (с.57 авт. та ін. всюди по тексту); відповідно до Закону України «Про освіту» у назві теми дисертації та у багатьох місцях по її тексту та автореферату замість правильного терміну вищі навчальні заклади – вищі заклади освіти та ін.; а також невдалі висловлювання, наприклад, «… запроваджує міжнародні правові стандарти криміналізації кіберзлочинів» (с.5 авт), оскільки термін *криміналізація* означає залучення до сфери впливу представників злочинного світу, отже, запроваджувати для цього міжнародні правові стандарти є безглуздим; незрозумілим є термін «оптимальні дидактичні методи» (с.32); потребує пояснення та обґрунтування використання терміну «диверсифікаційні освітні траєкторії», оскільки термін диверсифікація зазвичай використовується стосовно інвестицій, ринків товарів і послуг та ін., але ніколи – відносно освітніх систем та їх складників.

Висновки по роботі.

Висловлені побажання і зауваження суттєво не знижують загальної позитивної оцінки проведеного Б.В. Бистровою наукового дослідження.

На основі аналізу дисертації, автореферату і публікацій здобувача вважаю, що дисертаційне дослідження Бистрової Богдани Василівни „Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США”, є завершеним самостійним науковим дослідженням актуальної теми, що виконано на достатньому теоретико-методологічному рівні. Зміст дисертації відповідає спеціальності, за якою вона подана.

Висновки по розділах роботи та загальні висновки дисертації відповідають основному змісту дослідження та співвіднесені із завданнями.

Зміст автореферату ідентичний основним положенням дисертації та з необхідною повнотою відображає основний зміст, наукові положення і практичні результати дисертаційного дослідження.

Матеріали дослідження дають підстави для висновку, що поставлені автором завдання розв’язані, мета – досягнута.

Висновки й узагальнення, що отримані, навчально-методичний інструментарій, що застосовувався, збагачують дидактику вищої школи України

новими ідеями та положеннями в частині, яка стосується питань підготовки бакалаврів з кібербезпеки у закладах вищої освіти України.

Результати дослідження можуть бути використані викладачами відповідних дисциплін для вдосконалення навчального процесу підготовки бакалаврів з кібербезпеки у закладах вищої освіти України та у процесі підвищення кваліфікації професорсько-викладацьких та керівних кадрів у системі післядипломної освіти.

Загальний висновок

За своєю актуальністю, змістом, вірогідністю, новизною й практичною значущістю отриманих результатів дисертаційна робота **Бистрової Богдани Василівни** „Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США", подану на здобуття наукового ступеня кандидата педагогічних наук зі спеціальності 13.00.04 – теорія і методика професійної освіти, відповідає вимогам пунктів 9, 11, 12, 13, 14 „Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, та іншим нормативним вимогам, що висуваються до дисертаційних робіт на здобуття наукового ступеня кандидата наук, а її авторка заслуговує присудження наукового ступеня кандидата педагогічних наук зі спеціальності 13.00.04 – теорія та методика професійної освіти.

Офіційний опонент –
доктор технічних наук, професор,
дійсний член НАПН України,
директор Інституту інформаційних технологій
і засобів навчання НАПН України В.Ю. Биков